EIB Group Personal Data Protection Policy

November 2020

European Investment Bank Group

EIB Group Personal Data Protection Policy

November 2020

I. Introduction

1. Purpose, scope and applicability

The European Investment Bank Group consists of the European Investment Bank (EIB) and the European Investment Fund (EIF). In the following sections of this Policy, the term "Institution(s)" refers to the EIB and the EIF.

The EIB and the EIF place great importance on the protection and appropriate processing of personal data, including the personal data of its staff, clients, partners and suppliers. All staff members of the EIB and the EIF, employees, agents, contractors or consultants, as well as members of its governing bodies, should be made aware of the importance of processing and protecting personal data according to applicable laws and regulations.

This Policy defines the general data protection principles applied by both Institutions and shall be made publicly available on their respective websites.

This Policy applies to all personal data processing activities and related parties processing this data, including the Institutions' employees, contractors, vendors, service providers, partners, affiliates, volunteers and/or third-party organisations.

2. Document ownership, maintenance and review

Both the EIB and the EIF are responsible for owning and maintaining this Policy, whereas the Data Protection Officers are responsible for advising and guiding their respective Institutions. The review of this Policy will be carried out by the EIB and the EIF every three years if significant changes occur in order to ensure the Policy's continuing stability, adequacy and effectiveness.

II. Protection policy

1. Principles relating to processing of personal data

Both the EIB and the EIF shall ensure that all processed personal data are:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. Data protection policies and procedures

Each Institution shall create and maintain an inventory of policies/procedures related to the protection of personal data.

Each Institution shall adopt the following Procedures:

- Personal data breach management procedure;
- Procedure for the exercise of data subjects' rights;
- Data Protection Impact Assessment Procedure;
- Implementing Rules concerning the tasks, duties and powers of the Data Protection Officer in accordance with Article 45(3) of the Regulation[1,2].

3. Roles and responsibilities

Each Institution shall clearly define and allocate the roles and responsibilities with regard to the processing of personal data, especially for controllers and processors.

Should the EIB or the EIF act as processor on behalf of the other, a data processing agreement will be required.

---

1 https://www.eif.org/data-protection.

2 https://www.eib.org/publications/data-protection-implementing-rules.

In the event of joint controllership, the Institutions shall determine through a specific arrangement their respective responsibilities for compliance with their data protection obligations.

In addition, each Institution shall ensure that controllers shall be responsible for, and be able to demonstrate compliance with, the principles laid down in this Policy ('accountability').

4. Data Protection Officer

The EIB and EIF shall each formally designate a Data Protection Officer (DPO) for their respective Institution. Their tasks and responsibilities shall also be clearly set and documented in accordance with the Regulation. Inter alia, each Institution, in order to strengthen the DPOs' independence, shall ensure that the respective Data Protection Officer:

a) is involved, properly and in a timely manner, in all issues which relate to the protection of personal data;

b) does not receive any instructions regarding the exercise of his or her tasks; and

c) directly reports to the highest management level of the controller or the processor.

In accordance with the Memorandum of Understanding between the EIB and the EIF regarding the replacement of the Data Protection Officers of the EIB and the EIF, the DPO of the EIB and the DPO of the EIF shall act as a back-up for each other for the respective Institution, whenever either of them is absent or otherwise unable to fulfil his or her tasks.

5. Record of personal data processing activities

Each Institution shall create and maintain its own centralised register containing the records of processing activities carried out by both controllers and processors, when the EIB[3] or EIF[4] act as such.

6. Incident handling/personal data breach

The EIB and the EIF shall define an incident response plan to ensure an effective and orderly response to incidents pertaining to personal data, in particular personal data breaches. In addition, the DPOs of each Institution will create and maintain a record of personal data breaches.

7. Data Protection Impact Assessment

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. The controller shall seek the advice of the Data Protection Officer when carrying out a Data Protection Impact Assessment. The DPOs of each Institution will create and maintain a record of processes subject to a DPIA.

[3] https://www.eib.org/privacy/dpo-public-register.htm.

[4] https://www.eif.org/attachments/20201117-eif-records-of-processing-activities-ropa.pdf.

8. Confidentiality of personal data and training

Each Institution under the guidance of their respective DPOs shall ensure that employees involved in personal data processing activities are adequately informed about relevant data protection security measures, requirements and legal obligations through regular awareness campaigns. Employees of each Institution who are involved in high risk processing of personal data shall be bound to specific confidentiality clauses (under their employment contract or other legal act).

9. Technical security measures

Each Institution shall define and implement the adequate technical security measures to ensure the protection of personal data at each stage of its lifecycle: creation, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

EIB Group Personal Data Protection Policy

November 2020

European Investment Bank
98 -100, boulevard Konrad Adenauer
L-2950 Luxembourg
+352 4379-22000
www.eib.org – **info@eib.org**